Privacy policy web app

1. Information on the collection of personal data

1.1 We offer a web application ("web app") that you can access and use via your browser (mobile and desktop). This privacy policy describes how we collect, use and share your personal data when you use the web app. In this way, we would like to inform you about our processing procedures and fulfil our legal obligations, in particular those arising from the EU General Data Protection Regulation (GDPR).

1.2 Personal data is all data that can be related to you personally, e.g. image data (processed pseudonymised), skin condition metrics, skin type, product recommendations, gender, age, IP address and email address.

1.3 The controller within the meaning of Art. 4 (7) GDPR is Thea Care GmbH, Winterfeldtstraße 21 c/o Reaktor, 10781 Berlin, support@theacare.de (see our legal notice at www.theacare.de/imprint) (hereinafter also referred to as "we", "us" or "our").

2. Your rights

2.1 You have the following rights vis-à-vis us with regard to your personal data:

2.1.1 Right of access (Art. 15 GDPR),

2.1.2 Right to rectification (Art. 16 GDPR),

2.1.3 Right to erasure (Art. 17 GDPR),

2.1.4 Right to restriction of processing (Art. 18 GDPR),

2.1.5 Right to data portability (Art. 20 GDPR),

2.1.6 Right to object to processing (Art. 21 GDPR),

2.1.7 Right to protection from automated decision-making (Art. 22 GDPR),

2.1.8 Right to revoke the declaration of consent under data protection law, and

2.1.9 Right to lodge a complaint with a supervisory authority about the processing of your data by us.

3. Processing of personal data when using the web app

3.1 When you use our web app for purely informational purposes, i.e. when you use our web app without registering or otherwise providing us with information, we automatically collect the following personal data that your device transmits to our server and store it in log files:

3.1.1 IP address,

3.1.2 Date and time of the enquiry,

3.1.3 Time zone difference to Greenwich Mean Time (GMT),

3.1.4 requested file (page visited),

3.1.5 Page from which the file was requested (previously visited page),

3.1.6 Access status/HTTP status code,

3.1.7 amount of data transferred,

3.1.8 information about the browser type, language and version of the browser software, and

3.1.9 your operating system.

3.2 This data is technically necessary to display our web app to you and to ensure the stability and security of the system.

3.3 The legal basis for the processing of the aforementioned data is Art. 6 para. 1 sentence 1 lit. f GDPR. Our legitimate interest lies in the provision of a functional and secure web app.

3.4 The data is deleted as soon as it is no longer required to fulfil the purpose for which it was collected, at the latest after fourteen days.

3.5 If you use the skin analysis in our web app, we process various personal data. This processing is carried out for different purposes, each with a separate legal basis. Data processing is always pseudonymised.

3.5.1 Carrying out the skin analysis

Purpose: Analysis of your skin and creation of a skin profile (e.g. skin type, skin condition), including personalised product recommendations.

Processed data: Pseudonymised image data (technically rendered unrecognisable: e.g. eyes, mouth, background); skin type & skin condition metrics; perceived gender; perceived skin age; product recommendations

Legal basis: Art. 6 para. 1 lit. **b** GDPR (fulfilment of contract - performance of the requested analysis)

Storage period: The data is only processed for the duration of the session and then deleted. Any storage beyond that only takes place for other purposes and only with separate consent: image data for the further development of our AI (see section 3.5.3) and analysis results for marketing purposes (see section 3.5.4).

3.5.2 Receive result by e-mail

Purpose: Sending the analysis result to your e-mail address (on request)

Processed data: E-mail address (only for sending purpose); analysis result + product recommendation (temporarily in e-mail content)

Notes: Sent via processor Resend, server in the EU (Ireland); automatic deletion after 24 hours - no storage by us

Legal basis: Art. 6 para. 1 lit. **f** GDPR (legitimate interest in fulfilling a user request)

Storage period: The data is automatically deleted at the latest 24 hours after sending.

3.5.3 Use for research purposes (AI further development)

Purpose: Further development of our AI-supported skin analysis algorithms

Processed data: Pseudonymised image data

Legal basis: Art. 6 para. 1 lit. a i. V. m. Art. 9 para. 2 lit. a GDPR (consent to the processing of special categories of personal data)

Voluntary: Consent is voluntary. The skin analysis can be used without it.

Storage period: For a maximum of 36 months from the time consent was given, after which the data is deleted. If consent is withdrawn, the data is deleted without undue delay, even before this period ends.

Withdrawal: Possible at any time with effect for the future, by e-mail to support@theacare.de. As the stored image data is not linked to a name or e-mail address, the brand or web app address used (e.g. Nailvision or hautanalyse.nailvision.de) and the date and approximate time of the skin analysis (incl. time zone) are required to identify it. If these details match several images, all matching images are deleted.

3.5.4 Storage of your e-mail for marketing purposes

Purpose: Sending personalised product recommendations and offers

Processed data: E-mail address; analysis results (linked to e-mail address)

Notes: Stored in Supabase (server location: Frankfurt, EU); only with active consent; cancellation possible at any time

Legal basis: Art. 6 para. 1 lit. **a** GDPR (consent)

Storage period: Until you withdraw your consent or the contract is terminated.

3.5.5 If you log in to our web app as an employee or administrator, we also process the following data:

Purpose: Management of user access and provision of the administrative functions of the web app

Processed data: E-mail address; password (stored in encrypted form)

Notes: Login via processor **Clerk Inc;** processing takes place exclusively in the EU (Frankfurt); only accessible to registered employees or partners

Legal basis: Art. 6 para. 1 lit. **b** GDPR (fulfilment of contract); Art. 6 para. 1 lit. **f** GDPR (legitimate interest in secure access control)

Storage period: Until deletion of the user account or termination of the business relationship

4. Access rights of the web app

4.1 To be able to use the web app to its full extent, the web app requires at least one of the following access rights to your end device

4.1.1 Camera

4.1.2 Access to images/photo gallery (if user uploads a photo from the end device)

4.2 These authorisations are required to enable you to use the skin analysis function. Without this access, it is not possible to analyse your skin via the web app.

4.3 The legal basis for this data processing is our legitimate interest pursuant to Art. 6 para. 1 lit. f GDPR to provide a functional web app, your consent pursuant to Art. 6 para. 1 lit. a GDPR and § 25 para. 1 TTDSG, as well as the fulfilment of our contractual obligations pursuant to Art. 6 para. 1 lit. b GDPR (if a contract has been concluded).

5. Data security

We use appropriate technical and organisational measures to protect your data from manipulation, loss, destruction or unauthorised access. In doing so, we take into account the state of the art, the implementation costs and the type, scope, context and purpose of the processing. We also regularly assess the risks of a potential data breach, including its probability and impact. Our security measures are continuously adapted to technological progress.

6. Objection to or revocation of data processing

6.1 If you have consented to the processing of your data, you can revoke this consent at any time. The revocation applies from the time you notify us and affects the future processing of your data. The lawfulness of the processing of your data until your cancellation remains unaffected.

6.2 If we process your personal data on the basis of a balancing of interests, you can object to this processing. We carry out a balancing of interests in particular if we process your data in the public interest or on the basis of our legitimate interests. In your objection, please let us know the reasons why you object to the processing

of your data in its current form. We will examine your objection and will either discontinue or adapt the processing or explain to you our compelling reasons that justify the continuation of the processing.

6.3 Of course, you can object to the processing of your personal data for advertising and data analysis purposes at any time.

6.4 Please contact us for an objection or cancellation at support@theacare.de.

7. Storage duration of your personal data

7.1 We only store your personal data for as long as is necessary to fulfil the purposes for which it was collected. This includes the fulfilment of legal, tax and accounting obligations. In determining the retention period, we consider the amount, nature and sensitivity of the data, the potential risk of unauthorised use or disclosure, the purposes of the processing, whether we can achieve those purposes through other means and legal requirements.

7.2 In some cases, we will anonymise your personal data so that it can no longer be associated with you. In this case, we will use this data without further notification from you.

7.3 If you have any questions about the storage of your personal data, please contact us at support@theacare.de.

8. Data processing by third parties

8.1 We commission external service providers to process your data, e.g. service providers for the operation of the web app, for the processing of data or for the processing of payments. We select these service providers carefully, bind them to our instructions and monitor them regularly. We use the following third-party providers to provide and optimise certain functions of our web app

8.1.1 AWS Amplify & CloudWatch (Amazon Web Services EMEA SARL)

Purpose of processing: Operation and monitoring of the web app; processing of technical log data (e.g. IP address, access times)

Location of the processing: EU Central-1 (Frankfurt)

Legal basis: Art. 6 para. 1 lit. f GDPR (legitimate interest - system operation and security)

Further information: https://aws.amazon.com/privacy/

8.1.2 AWS S3 (Amazon Web Services EMEA SARL)

Purpose of processing: Storage of pseudonymised image data for skin analysis and AI further development

Location of the processing: EU Central-1 (Frankfurt)

Legal basis: Art. 6 para. 1 lit. a i. V. m. Art. 9 para. 2 lit. a GDPR (consent to the processing of special categories of personal data)

Further information: https://aws.amazon.com/privacy/

8.1.3 Supabase, Inc.

Purpose of processing: Storage of analysis results and email addresses with active marketing consent

Location of processing: EU Central-1 (Frankfurt)

Legal basis: Art. 6 para. 1 lit. a GDPR (consent for marketing and analysis purposes)

Further information: https://supabase.com/privacy

8.1.4 Resend (Plus Five Five, Inc.)

Purpose of processing: One-time sending of the analysis result by e-mail

Location of processing: EU West-1 (Ireland)

Legal basis: Art. 6 para. 1 lit. f GDPR (legitimate interest - dispatch on request)

Further information: https://resend.com/legal/privacy-policy

8.1.5 Clerk, Inc.

Purpose of processing: Provision of the login function for employees / partners; administration of registered users

Location of the processing: EU Central-1 (Frankfurt)

Legal basis: Art. 6 para. 1 lit. b and lit. f GDPR (contract fulfilment and access security)

Further information: https://clerk.com/legal/privacy

8.2 The legal basis for the transfer is then Art. 6 para. 1 sentence 1 lit. b or lit. f GDPR or, if consent has been requested, your consent pursuant to Art. 6 para. 1 sentence 1 lit. a GDPR. You can withdraw your consent at any time. The revocation applies from the time you notify us and affects future processing. The lawfulness of the processing until your cancellation remains unaffected.

8.3 Section 7 (Storage period) applies to the storage period.

8.4 If our service providers are based outside the European Union (so-called third countries), we will inform you about this in the respective functional description below. According to the European Commission's adequacy decision, some third countries have a level of data protection comparable to that in the EU. A list of these countries and copies of the adequacy decisions can be found here: https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en. In other third countries to which personal data may be transferred, a consistently high level of data protection may

be lacking. In such cases, we ensure that data protection is sufficiently guaranteed, e.g. through standard contractual clauses of the European Commission in accordance with Art. 46 para. 1, para. 2 lit. c GDPR.

9. Use of cookies

9.1 **General**: In addition to the data already mentioned, we use technical tools such as cookies, which are stored on your end device. When you visit our web app and also later, you can choose whether you want to allow cookies in general or select individual functions. You can customise these settings via our Cookie Consent Manager.

9.2 **What are cookies?** Cookies are small text files or database entries that are stored on your end device. They contain a characteristic string of characters that enables the web app used to be uniquely identified. Cookies cannot execute programmes or transmit viruses. Their main purpose is to make the use of our web app faster and more user-friendly. Below we explain the different types of cookies we use, how they work, how long they are stored and the legal basis for this.

9.2.1 **Technically necessary cookies**: We use necessary cookies for the technical operation of our web app. Without these, the web app cannot be displayed completely or correctly and certain support functions would not be available. These cookies are usually temporary cookies (see below for an explanation of the term). These cookies cannot be deselected if you wish to use our web app. You can find an overview of these cookies in the Cookie Consent Manager. The legal basis for this processing is Art. 6 para. 1 sentence 1 lit. f GDPR.

9.2.2 **Technically optional cookies**: We only set these cookies with your consent, which you can give via the Cookie Consent Manager when you first visit our web app. They enable us to analyse and improve the use of the web app, facilitate operation via various end devices, recognise you when you visit again or place advertising that is tailored to your interests and measure its effectiveness. The legal basis for this processing is Art. 6 para. 1 sentence 1 lit. a GDPR. You can revoke your consent at any time.

9.3 **Storage duration**: The storage duration depends on whether the cookies are temporary or persistent (permanent) cookies.

9.3.1 **Temporary cookies**: Such cookies, especially session cookies, are automatically deleted when the web app is closed or when you log out. They contain a so-called session ID. This allows various requests from your end device to be assigned to the shared session and your end device can be recognised when you return to our web app.

9.3.2 **Persistent cookies**: These are automatically deleted after a specified period, which varies depending on the cookie.

10. Online marketing / analysis tools

10.1 We use online marketing and analysis tools to design our web app to meet your needs and to continuously optimise its use. These measures are based on your consent in accordance with Art. 6 para. 1 sentence 1 lit. a GDPR. If data is transferred to a country outside the European Union (so-called third country), this is done if you have expressly consented to this or if it is necessary for the provision of our services to you or if it is provided for by law (Art. 49 GDPR). Your data will only be processed in third countries if an adequate level of data protection is ensured by certain measures, e.g. by an adequacy decision of the EU Commission or by suitable guarantees in accordance with Art. 44 et seq. GDPR.

10.2 Google Analytics

10.2.1 If you have given your consent, we use Google Analytics 4 on this website, a web analytics service provided by Google LLC. For users in the EU, the EEA and Switzerland, the controller is Google Ireland Limited, Dublin, Ireland ("Google"). Google Analytics enables us to analyse the behaviour of website visitors. In doing so, we receive various usage data such as page views, length of visit, operating systems used and the origin of the users.

The data processing is based on your consent in accordance with Art. 6 para. 1 sentence 1 lit. a GDPR. You can withdraw your consent at any time.

10.2.2 The data collected by Google Analytics is generally transferred to a Google server in the USA and stored there. The European Commission issued an adequacy decision for data transfers to the USA on 10 July 2023. Google LLC is certified under the EU-US Data Privacy Framework. In addition, we have concluded the EU standard contractual clauses with Google.

10.2.3 IP anonymisation is activated by default in Google Analytics 4. This means that your IP address is truncated within the EU or EEA before it is transmitted to Google. Only in exceptional cases will the full IP address be transferred to the USA and truncated there. According to Google, the IP address transmitted by your browser will not be merged with other Google data.

10.2.4 We use the User ID function. With the user ID, we can assign a unique, permanent ID to several sessions and thus analyse user behaviour across devices.

10.2.5 We use Google Signals. With Google Signals, we collect additional information from users who have activated personalised ads (e.g. interests and demographic data). This data can be used across devices for personalised advertising.

10.2.6 During your visit to the website, your user behaviour is recorded in the form of 'events'. These include, for example, page views, first visit to the website, start of the session, web pages visited, your 'click path', interactions with the website, scrolling actions, clicks on external links, internal search queries, interactions with videos, file downloads, adverts viewed or clicked on and your language setting.

10.2.7 In addition, your approximate location (region), date and time of the visit, your IP address (in abbreviated form), technical information about your browser and the end devices used (e.g. language setting, screen resolution), your internet provider and the referrer URL (via which website or advertising medium you came to this website) are recorded.

10.2.8 You can prevent the installation and storage of cookies by setting your browser software accordingly; however, we would like to point out that in this case you may not be able to use all functions of this website to their full extent.

10.2.9 You can also prevent the collection of data generated by the cookie and related to your use of the website (including your IP address) and the processing of this data by Google by downloading and installing the browser plugin available at the following link: https://tools.google.com/dlpage/gaoptout?hl=de.

10.2.10 You can deactivate the use of your personal data by Google using the following link: https://myadcenter.google.de/personalizationoff

10.2.11 We have concluded a data processing agreement (DPA) with Google to ensure that your personal data is only processed in accordance with our instructions and in compliance with the GDPR.

10.3 **Google Tag Manager**

10.3.1 Google Tag Manager, provided by Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Ireland ("Google"), is a tool that enables us to integrate tracking and statistics tools and other technologies on our website. The tool itself does not create any user profiles, does not store any cookies and does not carry out any analyses of its own. It is only used to manage and display the integrated tools. The Google Tag Manager records your IP address, which may also be transmitted to Google in the USA.

10.3.2 The data collected by Google is usually transferred to a Google server in the USA and stored there. The European Commission issued an adequacy decision for data transfers to the USA on 10 July 2023. Google LLC is

certified under the EU-US Data Privacy Framework. In addition, we have concluded the EU standard contractual clauses with Google.

10.3.3 The use of Google Tag Manager is based on Art. 6 para. 1 sentence 1 lit. f GDPR. Our legitimate interest lies in the efficient management of various tools on the website. If consent has been obtained, the processing is carried out on the basis of Art. 6 para. 1 sentence 1 lit. a GDPR and § 25 para. 1 TTDSG. You can withdraw your consent at any time.

10.3.4 Further information on Google Tag Manager and Google's privacy policy can be found at https://policies.google.com/privacy?hl=de and https://marketingplatform.google.com/about/analytics/tag-manager/use-policy/.

10.3.5 We have concluded a data processing agreement (DPA) with Google to ensure that your personal data is only processed in accordance with our instructions and in compliance with the GDPR.

10.4 Google Ads / Google Conversion Tracking

10.4.1 We also use the online advertising programme "Google Ads" and conversion tracking as part of Google Ads, provided by Google Ireland Limited, Dublin, Ireland ("Google").

10.4.2 Google Ads enables us to display adverts for certain search terms or based on user data such as location and interests. We can also analyse this data, e.g. which search terms triggered ads and how many clicks they achieved.

10.4.3 Google Conversion Tracking enables us to recognise whether users have performed certain actions on our website, such as clicking on buttons or purchasing products. This data helps us to compile conversion statistics. We find out the number of users who have clicked on our adverts and what actions they have taken, but without personal identification. Google uses cookies or similar technologies for this purpose.

10.4.4 The data collected by Google is generally transferred to a Google server in the USA and stored there. The European Commission issued an adequacy decision for data transfers to the USA on 10 July 2023. Google LLC is

certified under the EU-US Data Privacy Framework. In addition, we have concluded the EU standard contractual clauses with Google.

10.4.5 The use of Google Ads and Google Conversion Tracking is based on your consent in accordance with Art. 6 para. 1 sentence 1 lit. a GDPR. You can withdraw your consent at any time.

10.4.6 Further information on Google Tag Manager and Google's privacy policy can be found at https://policies.google.com/privacy?hl=de.

10.4.7 We have concluded a data processing agreement (DPA) with Google to ensure that your personal data is only processed in accordance with our instructions and in compliance with the GDPR.

10.5 Posthog

10.5.1 We use the open source tool PostHog for anonymised analysis of user behaviour in our web app. Processing only takes place with your consent (analytics cookie). IP addresses, text entries, images and geodata are not recorded or completely masked by technical settings.

10.5.2 Processing takes place exclusively on servers within the European Union. Profiling or user identification does not take place.

Purpose of processing: Improving user-friendliness and analysing usage

Location of the processing: EU Central-1 (Frankfurt)

Legal basis: Art. 6 para. 1 lit. a GDPR (consent)

Further information: https://posthog.com/privacy

11. Making contact by e-mail

When you contact us from the web app (e.g. by e-mail or via a contact form), the data you provide (your e-mail address, your name and telephone number if

applicable) will be stored by us in order to answer your questions. Data processing for the purpose of contacting us is carried out in accordance with Art. 6 para. 1 sentence 1 lit. a GDPR on the basis of your voluntarily given consent. If the enquiry is assigned to a contract, we delete the data arising in this context after the contract period has expired, otherwise after storage is no longer necessary, or restrict processing if there are statutory retention obligations.

12. Up-to-dateness of and changes to this privacy policy

It may become necessary to amend this privacy policy as a result of the further development of our web app and offers or due to changes in legal or official requirements.

Status: 16.09.2026